30 November 1978

STAT MEMORANDUM FOR: [redacted]
Special Assistant to the DCI

STAT FROM: [redacted]
Chief, Community Security Group

SUBJECT: Compartmentation

1. As we approach implementation of the proposals to revamp the compartmentation programs, it is desirable that certain security terms be defined in common. Terms with specific meaning and application in the security environment include clearance, access approvals, Compartmentation Security Control Systems. It would also be appropriate to see how these terms fit into the scheme of things at this stage of the revision. Lastly, it may be of interest to offer comment from my seat as your security advisor.

2. We should agree on the following definitions:

a. Clearances -- There are only three clearances in the U.S. Government. They correspond to the permissible levels of classification of Confidential, Secret and Top Secret. E.O. 10450 provides guidance on what is required for an individual to be given a clearance at the various levels. Once an individual is cleared for a given level of classified material, he is potentially a recipient of all material classified at that level. Whether he gets access to the material is not a function of "clearance" but of the application of a different set of rules defined as "need-to-know".

78/112

b. Access Approvals - An access approval is an action, either tacet or specific, leading to a determination that an individual should be granted access to specific material. They are different than "clearances". TALENT-KEYHOLE or TKH is the name of an access approval. It is also the name of a compartmentation control system established to protect the products from space reconnaissance. SI Category I, II or III are the names of the access approvals to material of the same designation in the COMINT Control System. GAMMA is the name of both the access approval and the GAMMA Control System. [redacted] etc., are names of access approvals to specific projects protected in the [redacted] Security Control System. [redacted] is the name of Security Control System. [redacted] is the name of the access approval to a specific project within the [redacted] Control System. The product of this project/operation is protected by a separate control system called [redacted] is also the name of the access approval for access to this product. For our purpose, let's define an access approval as a documented need-to-know that requires three actions:

(1) A determination that the individual meets the personnel security criteria of DCID 1/14.

(2) A written statement of "need-to-know" by an officer authorized to grant access. In most cases a statement of justification is to be prepared and submitted to the Program Manager and the SIO. If satisfied, they sign authorization for access subject to;

(3) execution of a signed secrecy agreement which spells out the terms of what is to be kept secret.

c. Compartmentation Control System - Executive Order 12065 defines these as Special Access Programs to control access, distribution and protection of sensitive information classified pursuant to this Order or prior Orders. E.O. 12065 sets out guides as to when these Special Access Programs may be created or continued. They include requirement of specific showings that normal management and safeguard procedures are not sufficient to limit need-to-know or access, members will be reasonably small and protection and needs for access balance. Such programs may be created or continued only by written direction of the Director of Central Intelligence for matters pertaining to intelligence sources and methods. The programs have to be reviewed regularly and terminate automatically every five years unless renewed.

3. Looking at application of these concepts to the current status of efforts to reorganize our compartmentation programs reveals a few anomalies and merits a few security observations:

a. We have been informed by counsel that any level of classified material can be compartmented. Therefore, material at the Confidential, SECRET or TOP SECRET level can be nominated for compartmentation. However, our proposals are silent about the requirement that recipients must have the appropriate level of clearance to receive our compartmented classified material. This can be fixed by inclusion of a requirement that individuals must first possess an appropriate clearance for access to the classified material we have placed in compartmentation.

b. The current proposal is silent on the conditions of need-to-know other than that agreement between collectors and SIO's is required on who shall have access. I propose that we flesh this out and require that proposed recipients be identified individually by name. This security recommendation is not to dismiss any advantage of using a billet system to assist in arriving at who will have a "need-to-know". It is meant to assure that individuals and not positions are granted a need-to-know.

c. Application of the definition of Access Approval requires that we include the additional provision of DCID 1/14 as a personnel security criteria and execution of a secrecy agreement as conditions precedent to access to compartmented intelligence.

d. Identifying all compartmented intelligence under the umbrella term APEX permits a simple means of identifying the material differently than non-compartmented material. It offers the advantage of establishing a single access approval which could also be called APEX. The proposal has the further advantage of permitting publication of all source finished intelligence with a single identifier. These three conditions would further efforts toward the aims of the revised concept of compartmentation with the exception that it would not offer a more disciplined implementation of the "need-to-know" or assist in controlling or managing access to compartmented information and finished intelligence. My reasons for this position stem from the belief that we do not know the size of the population that would have a "need-to-know" but that all individuals authorized access to APEX material would have potential access to all of it. The proposal would permit COMINT, ELINT, TECHINT and IMAGERY to be placed in APEX without means of administratively controlling who had access to what. It reduces the possibility of controlling access to these categories. We would not have the seven clearances [redacted] proposed or the revised proposal of a system with four categories of information controlled on a "must know" basis by SIO's. We would have one large category of material and one access approval. I think this proposal fails to meet the requirement for balance between access and control. There would be too much access and too little control.

STAT

I appreciate the desire to arrive at an accommodation to facilitate dissemination of all sources finished intelligence but granting across the board access to all consumers of finished intelligence defeats the very purpose of compartmentation. I see no easing of security concerns in the claims that the volume of such material will be small and that access would be contingent upon strict application of "must know". In support, I point to the marked increase in the size of the dissemination list of the all source NID. Originally small and tightly controlled, the recipients now number in the hundreds and the NID is just another intelligence report received on a daily basis. However, if the concept is pursued, carefully considered security controls would have to be adopted.

4. The presentation before NFIB with subsequent adoption and anticipated member support of the revised proposals on compartmentation should assist in determining just what will have to be implemented. Security elements throughout the Community have assured their complete support.

[redacted] STAT